Appendix 16
SDS Information Security Policy for NTP Providers

Background and Purpose

The purpose of this document is to outline the required behaviour of Providers when using the Skills Development Scotland (SDS) IT systems and handling personal data. The rules are defined to protect the interests of SDS, the organisations contracted to deliver National Training Programmes on behalf of SDS and the programme participants. The intention is not to impose intrusive constraints that are contrary to our established culture of openness, trust and integrity, which SDS recognise as essential contributors to the success of SDS. Information Security is committed to protecting the operation and reputation of SDS in fulfilling its role as the catalyst for real and positive change in Scotland's skills performance. This document applies to all National Training Programme information processed by and on behalf of SDS.

Responsibility

- All organisations contracted to deliver National Training Programmes are responsible for implementing, enforcing and adhering to the provisions of this policy.
- All contract signatories are responsible for ensuring this policy is adhered to.
- All company employees are responsible for ensuring visitors are also aware of this policy and are supervised appropriately.

Policy

Any Provider in breach of this policy will be in breach of the Provider Contract with SDS and may have their contract terminated.

Policy Statements

SDS IT System Access

1. The SDS IT systems are accessed using your own individual SDS login id and password. Do not leave clues or evidence of passwords near to your computer. Passwords should be minimum of 8 characters and include at least 3 of the following:
    a. Capital letter
    b. Small letter
    c. Number character
    d. Special characters (?$%&*)
2. Using another person's login id is not permitted under any circumstances.
3. Some SDS IT systems require the use of multi factor authentication. This relies on additional security of a separate device / system such as a mobile phone or email account. In the event that the separate system is compromised or the device lost providers must notify SDS.
4. Passwords must not be saved on any login screen, e.g. do not tick 'Save Password' or 'Remember Me' options if these appear.
5. Never leave a logged-in computer unattended when using SDS IT systems. Use the Windows (or operating system equivalent) 'Lock Workstation' facility (Windows key + L) or logout.
6. Protect against accidental compromise of SDS and participant information; ensure information cannot be observed by unauthorised people.
7. Deliberate, unauthorised entry to SDS IT systems, entry of false data and unauthorised changes to information are strictly forbidden.

8. Providers must report all security incidents. In the first instance please contact your SDS assigned Skills Investment Advisor who will ensure the correct handling of the incident.
9. Data extracted or originating from SDS IT systems must be encrypted or transferred in a secure manner when forwarding to SDS.
10. Providers must promptly inform SDS if they no longer need access to SDS systems.
11. Providers are required to comply with the terms of the FIPS licensing agreement in place between them and SDS.

Electronic Data Transfer – Mandatory Data Encryption

12. Data Encryption is a mandatory requirement of SDS where personal data is being transferred from and to third party organisations including Providers. SDS currently utilise WinZip to encrypt files with 256 bit AES encryption. All data transfers between SDS and third parties must use compatible encryption software (for WinZip version 9.0 and greater is compatible). Each data transfer will be to a named contact by means of an encrypted Zip file that will use the SDS assigned shared encryption password. The Shared encryption / decryption password is issued by SDS annually. The password must not be transmitted by the same means as the encrypted data file. Data transferred back to SDS must also be encrypted. The encrypted file may be transmitted by email. Where encrypted files cannot be transferred by this method they should be burned to CD and posted by registered mail and signed for or hand delivered. If encrypted files are not available, hard-copy documents must be posted by using double envelopes
13. The provider must ensure that any portable devices, such as Laptops and Tablets, which are used to store participant's personal information are encrypted.
14. It is the responsibility of the Provider to provide their own copy of the necessary encryption software.

Handling Hardcopy Documents and Electronic Media containing Personal Information

15. Providers are required to collect and store both personal information and sensitive personal information as defined by the Data Protection Act. This information must be securely protected to avoid the risk of data loss and unauthorised exposure.

Collecting

16. Personal information particularly 'sensitive' information must only be gathered from participants in an environment that respects their privacy and limits the opportunity for the trainees to be over looked.

Processing

17. When a provider processes a participant's personal data it should be done in a way to limit the opportunity for unauthorised access to the information.
18. Providers should consider protecting participants information from unauthorised viewing by:
    - observing a clear desk policy;
    - handling hardcopy in non transparent folder;
    - Ensuring that documents are not left at printers and copiers and
    - Ensuring only authorised staff have access to the information

Storage

19. When not in use hardcopy files with personal information must be stored in lockable filing cabinet or drawers.
20. At the end of the working day the filing cabinets and drawers containing the participant's personal information must be locked.

Sending

21. The preferred option for transferring personal information between parties is to use encrypted electronic communications as defined above in the section *Electronic Data Transfer – Mandatory Data Encryption.* If this is not available hardcopy documents can be exchanged either be posted using double envelopes or hand delivered.

Disposal

22. Prior to disposal of information providers should check the retention and archiving requirements.
23. Hardcopy document that are no longer required should be shredded or disposed off via a confidential waste contractor.
24. For electronic storage media these should be destroyed or overwritten sufficient that the data cannot be retrieved.
    - CD/DVD's shredded
    - Memory sticks – destroyed or formatted in a way that data cannot be recovered.

Data Loss or Compromise

25. Any incident of data being loss or compromised must be reported promptly to SDS CTS Compliance Team.